

# Information Security

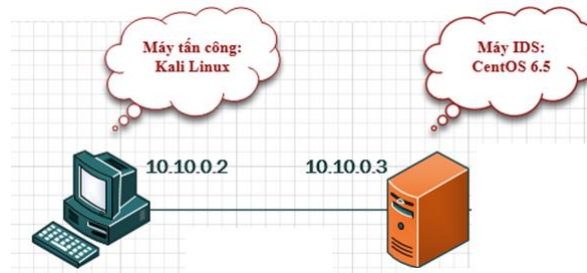
## Chapter 10: LAB - IDS/IPS

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

## Practice

- ☞ Set up an IDS using:
  - **Snort**
- ☞ Simulate attacks and use IDS above to detect
  - **Ping**
  - **DDOS**
  - **Brute Force**

# IDS



29/10/2024

3

# Process

- ☞ Set up IDS with Snort
  - Download and install Snort
  - Database: MySQL – install, create, GRANT....
  - Graphic Interface for Snort:
    - Web server, PHP
    - pear
    - ADODB: <http://nchc.dl.sourceforge.net/sourceforge/adodb/>
    - BASE: <http://nchc.dl.sourceforge.net/sourceforge/secureideas/base-1.4.2.tar.gz>
- ☞ Set up attacker machine (DOS, Brute Force,...)
  - **Test Ping:** ping
  - **DDOS:** hping3
  - **Brute Force** – using Hydra (telnet, ftp, http...)
  - **SQL Injection**

29/10/2024

4

## Cấu hình cơ bản

```
$ nano /etc/snort/snort.conf
ipvar HOME_NET <IP/subnetmask>
ipvar EXTERNAL_NET !$HOME_NET
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
```

29/10/2024

5

## Kiểm tra file cấu hình

```
$ snort -T -c /etc/snort/snort.conf
```

```

==== Initialization Complete ====

-*> Snort! <*-
Version 2.9.8.0 GRE (Build 229)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2015 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.7.4
Using PCRE version: 8.35 2014-04-04
Using ZLIB version: 1.2.8

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_DCEP2C2 Version 1.0 <Build 3>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>

Snort successfully validated the configuration!
Snort exiting
root@pc:~#
```

29/10/2024

6

# chạy Snort

```
$ /usr/local/bin/snort -A console -c /etc/snort/snort.conf -i eth0
```

```

_*> Snort! <*-
o"-)- Version 2.9.8.0 GRE (Build 229)
'-'-' By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014-2015 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.7.4
      Using PCRE version: 8.35 2014-04-04
      Using ZLIB version: 1.2.8

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_DCEPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>

Commencing packet processing (pid=4653)

```

29/10/2024

7

# ping

🔗 Create rule icmp – ping:

```
$ nano /etc/snort/rules/icmp.rules
```

```
alert icmp any any -> $HOME_NET any (msg:"Co ai do dang
ping"; sid:10000001; rev:001;)
```

🔗 Add rule path in **snort.conf**

```
$ nano /etc/snort/snort.conf
```

```
include $RULE_PATH /etc/snort/rules/icmp.rules
```

🔗 **At attacker:** ping <IP\_IDS>

🔗 **At IDS:**

```

Commencing packet processing (pid=4713)
12/26-22:46:12.921834  [**] [1:10000001:1] Co ai do dang ping [**] [Priority: 0] {ICMP} 192.168.1.17 -> 192.168.1.11
12/26-22:46:12.921884  [**] [1:10000001:1] Co ai do dang ping [**] [Priority: 0] {ICMP} 192.168.1.11 -> 192.168.1.17
12/26-22:46:13.911806  [**] [1:10000001:1] Co ai do dang ping [**] [Priority: 0] {ICMP} 192.168.1.17 -> 192.168.1.11
12/26-22:46:13.911851  [**] [1:10000001:1] Co ai do dang ping [**] [Priority: 0] {ICMP} 192.168.1.11 -> 192.168.1.17
12/26-22:46:14.878252  [**] [1:10000001:1] Co ai do dang ping [**] [Priority: 0] {ICMP} 192.168.1.17 -> 192.168.1.11
12/26-22:46:14.878272  [**] [1:10000001:1] Co ai do dang ping [**] [Priority: 0] {ICMP} 192.168.1.11 -> 192.168.1.17
12/26-22:46:15.872077  [**] [1:10000001:1] Co ai do dang ping [**] [Priority: 0] {ICMP} 192.168.1.17 -> 192.168.1.11
12/26-22:46:15.872118  [**] [1:10000001:1] Co ai do dang ping [**] [Priority: 0] {ICMP} 192.168.1.11 -> 192.168.1.17

```

🔗 Ref: <https://adminvietnam.org/cai-dat-snort-ids-tren-ubuntu/1210/>

29/10/2024

8

## dos

### 🔗 Create rule dos – **hping3**:

```
$ nano /etc/snort/rules/dos.rules. Ex:
  alert tcp any -> $HOME_NET 80 (msg:"DDOS GET";content:"GET /
  HTTP"; flow:to_server, established; threshold: type threshold,
  track by_src, count 30, seconds 30; sid:1000004;)
```

### 🔗 Add rule path in snort.conf

```
$ nano /etc/snort/snort.conf
  include $RULE_PATH/dos.rules
```

### 🔗 At attacker: hping3 ... <IP\_IDS>

### 🔗 At IDS:

```
....."DDOS GET"
```

29/10/2024

9

## Exercise (3)

### 🔗 Execute at least 3 attacks:

- **DDOS**: using hping3, slowloris,.....
- **Brute Force to crack password**: using Hydra (telnet, ftp, http...)
- **SQL Injection**: using DVWA, sqlmap

### 🔗 Using IDS Snort to detect attacks above

29/10/2024

10